Request for Proposals

Access Control and IP-based CCTV

The Woodlands Township
2201 Lake Woodlands Dr.
The Woodlands, Tx 77380

Deadline for Submittal:
Wednesday, April 13, 2011
No later than 3:00 P.M.

REQUEST FOR PROPOSALS (RFP)

Section I General Information

1. Purpose of Solicitation

This solicitation is a Request for Proposal(s) (RFP). The purpose is to solicit responses from qualified companies that describe their capabilities to identify, design, purchase, install, train, document, service and warranty an Access Control and IP based CCTV system for The Woodlands Township ("The Township"). This responding entity shall be prepared to perform the services listed in this RFP. Such services shall include a turnkey Access Control and CCTV system, as well as design and installation services that include the services listed in this request and meets the requirements of the described work.

2. Services Requested

The Township has commenced renovations of a facility that requires an Access Control and IP-CCTV system.

The Township currently maintains an IP-CCTV system; AXIS camera management 2.0 with Surveillance Manager 4.7, and includes 1 AXIS 213 camera and (10) AXIS 233 Cameras.

Respondents will determine whether it is cost effective to expand the current AXIS camera system or provide an alternate IP-CCTV proposal that shall be non-proprietary and readily available. Clearly note any improvements in performance, such as increased resolution.

Respondents to this RFP shall identify their experience and qualifications to perform analysis, design engineering, and installation of integrated an Access Control and IP-CCTV system as outlined in Section II below.

3. Buildings/Project Description

The following building will be involved in this Access Control and CCTV system.

The Woodlands Township, under renovation and construction at 2801 Technology Forest Blvd, The Woodlands, TX 77381 Montgomery County, comprised of one floor and totaling approximately 69,000 GSF.

4. Proposal Format

Proposals must be submitted in the format outlined in this document. Each proposal will be reviewed to determine if it is complete prior to actual evaluation. Proposals not containing all of the requested the information will not be considered and will be deemed non-responsive. Respondents shall use the prescribed format to indicate their experience and qualifications, to describe their approach to this project, and to explain their proposed contract.

5. Contract Responsibility

The selected provider will be required to assume total responsibility of the Access Control and CCTV portion of the project.

The provider must perform their work so that the system is substantially complete at the same time the building general contractor is substantially complete.

The provider may identify supplemental work, external to their contract scope, which must be performed by others to allow their proposed integrated system to be installed and to be fully functional.

The provider must coordinate, cooperate, and schedule their work, with The Township, Kirksey Architecture, and The Township's building general contractor, so that these supplemental work components can be implemented into the project.

6. SPECIAL PROVISIONS

A. **Financial Condition**

Firm must provide audited financial statements, if requested, to The Township.

B. **Reservations**

The Township reserves the right to accept or reject any or all Proposals as a result of this request, to negotiate with all qualified sources, or to cancel, in part or in its entirety, this Request for Proposal if found in the best interest of The Township. Additionally, although The Township desires to contract with a single firm for all work/services to be provided, The Township reserves the right to split the work/services and deal with multiple firms if it is deemed to be in The Township's best interest. All Proposals become the property of The Woodlands Township

C. **Contract Terms and Conditions**

It is understood that any resulting contract executed will contain the following Indemnification and Release language:

D. **Indemnification**

It is further agreed that the Contractor (separately and collectively the "Indemnitee") shall indemnify, hold harmless, and defend The Township, its officers, agents, and employees from and against any and all claims, losses, damages, causes of action, suits, and liability of every kind, including all expenses

of litigation, court costs, and attorney's fees, for injury to or death of any person or for damage to any property arising out of or in connection with the work done by the Contractor under this Contract. Such indemnity shall apply regardless of whether the claims, losses, damages, causes of action, suits, or liability arise in whole or in part from the negligence of The Township, any other party indemnified hereunder, the Contractor, or any third party.

E. **Patent and Copyright Indemnity:**

The Contractor will indemnify, defend and hold harmless The Township against any claim, legal suit or administrative proceeding, liability or judgment that the Hardware and Software used as authorized under this Agreement infringes U.S. patent, copyright or other proprietary right. The Contractor will indemnify The Township against all costs, damages and legal fees, expert fees and other related fees and expenses finally awarded provided that The Township promptly notifies the Contractor in writing of the claim; Contractor has sole control of the defense and of all related settlement negotiations; and The Township provides all reasonable assistance in such defense as may be reasonably requested by the Contractor. If the hardware or software becomes, or in the Contractor's opinion is likely to become, the subject of infringement, the Contractor shall, at its option and expense, either procure for The Township the right to continue using the hardware and software; or replace or modify the hardware and software so that it becomes non-infringing. If neither of the foregoing alternatives is reasonably available, The Township agrees that the Contractor shall have the right to terminate the Agreement and The Township shall promptly return to the Contractor the original copy and all other copies of the hardware/software after the Contractor pays to The Township an amount equal to a five year straight line depreciation based of the charge for the hardware/software. This Patent and Copyright Indemnity shall not apply to any claim based upon: the use of other than a current release of the hardware/software; the combination, operation or use of any hardware/software with other software or data; or the use of the hardware/software in other than the operating environment specified for it by the Contractor.

E. Release:

The Contractor assumes full responsibility for the work to be performed hereunder and hereby releases, relinquishes, and discharges The Township, its officers, agents, and employees from all claims, demands, and causes of action of every kind and character, including the cost of defense thereof, for any injury to or death of any person and any loss of or damage to any property that is caused by, alleged to be caused by, arising out of, or in connection with the Contractor's work to be performed hereunder. This release shall apply regardless of whether said claims, demands, and causes of action are covered in whole or in part by insurance and regardless of whether such injury, death, loss, or damage was caused in whole or in part by the negligence of The Township, any other party released hereunder, the Contractor, or any third party.

F. Warranty:

The Contractor warrants that it shall provide the work and services in accordance with the highest computer and computer consulting industry standards and practices applicable to its work and the error correction of any licensed software, training and advice to Customer during the performance of the services provided in accordance with the standard.

7. Required Insurance and Bonds

A. **Workers' compensation**: Contractor shall purchase and maintain Workers' Compensation Insurance with statutory limits in accordance with all applicable state, federal and maritime laws, and Employers' Liability Insurance of $1,000,000.00 per accident/occurrence, including, without limitation, an "Alternate Employer" and "Borrowed Servant" endorsement.

B. **Liability insurance**: Contractor shall purchase and maintain Commercial General Liability Insurance with $1,000,000.00 combined single limit for Bodily Injury and Property Damage, specifically including Contractual Liability for their respective obligations under this Agreement, including Products Liability.

C. **Automobile Liability Insurance**: If owned, hired, or non-owned automotive equipment is used in the performance of this Agreement, Contractor, as applicable, shall purchase and maintain Automobile Liability Insurance with $2,000,000.00 combined single limit for Bodily Injury and Property Damage, including, without limitation, Hired and Non-Owned Liability.

D. **Protection and Indemnity Insurance**: Contractor shall purchase and maintain Protection and Indemnity Insurance with limits of $1,000,000.00 combined single limit per occurrence, including but not limited to coverage for contractual liability for those liabilities assumed by the Party.

E. **Property Damage or Casualty Insurance**: Contractor shall purchase and maintain Property Damage Insurance on their respective property, whether real (including, without limitation, buildings and fixtures, as applicable) or personal (including, without limitation, equipment and tools) for its replacement cost. With respect to leased equipment, the Contractor shall make certain that either lessor or lessee of such leased equipment is covered by Property Damage Insurance.

8. Taxes, Fees, Code Compliance, Licensing

The provider shall be responsible for payment of any required taxes or fees associated with the contract. The provider shall be responsible for compliance with all applicable codes and laws in connection with performing the work contemplated under the contract.

9. Deliverables

The deliverables shall be accepted by The Township when (1) the deliverables have been delivered, installed and made ready for use at The Township's site in accordance with the installation and operating specifications; (2) The Township has tested the deliverables and the deliverables have passed testing; (3)The Township's designated staff have received system documentation and training;(4) The Township agrees that deliverables meet or exceed the specifications and those contained in the scope of work and order concerning performance and capabilities of the deliverables.

10. Acceptance Testing

Once the deliverables are installed in The Township's premises as specified herein with regard to the Final Installation Date, the Contractor shall notify The Township in writing that the deliverables as specified have been installed in good working order and ready for use, that the modifications or enhancements are completed as defined and specified herein, are in good working order, ready for use, and to the best of the Contractors knowledge is one hundred percent operational and that the deliverables as installed is ready for testing. At that point, The Township shall have thirty (30 working days to perform and complete acceptance testing on-site. If the deliverables as installed and represented passes such testing, The Township shall so notify the Contractor in writing termed the Certificate of Acceptance. If the deliverables as installed fails to pass such testing, The Township shall notify the Contractor in writing and the Contractor shall then have ten (10) working days to correct any failure. The Contractor shall then certify to The Township that the failure has been corrected and The Township shall have ten (10) working days for additional testing at which time The Township shall supply the Certificate of Acceptance if the deliverables passes testing. If the deliverables fails testing twice, at The Township's option: (1) the correction period may be extended as agreed by the parties; or (2) The Township may terminate the Agreement, return the specifications, product and documentation to the Contractor and the Contractor will refund to The Township any payments previously given to the Contractor for the deliverables and modifications or enhancement pursuant to the Agreement.

11. References and Proprietary Information

All proposers grant The Township permission to make inquiries concerning the respondent and its qualifications and references to any persons or firms deemed appropriate by The Township. Any proprietary information that the respondent provides in response to this RFP and for which provider does not want disclosed to the public shall be so identified on each page on which it is found. Data or information so identified will be used by The Township solely for the purpose of evaluation and contract negotiations. Disclosure of any of provider's proprietary information by The Township to third parties shall be in strict accordance with the laws and regulations regarding disclosure in the State of Texas.

12. Award

The Woodlands Township reserves the right to accept proposals, award proposals and/or not award proposals on individual items listed, on group items, or on the proposal as a whole; to reject any and all proposals, to waive any informality in the proposals, and to accept the proposal that appears from all consideration to be for the best interest of The Woodlands Township.

In determining and evaluating the best proposal, the prices will not necessarily be controlling, but quality, equality, efficiency, utility, general terms, delivery, suitability of the equipment/material offered, and the reputation of the equipment/material in general use will also be considered with any other relevant factors.

Notice of proposal award, if proposal be awarded, will be made within thirty (30) days of opening of proposals. The Township Board of Directors will authorize the selected respondent to commence performance of the work tasks set forth in the Final Proposal. Receipt of the official Purchase Order of The Woodlands Township covering the supplies, materials, equipment or services as described in the Proposal will indicate the award of the proposal and a contract to purchase; upon finalization of the Final Proposal between the selected respondent and The Township.

Section II
Format Requirements and Preparation Instructions

Proposals must be received on or before 3:00 PM, April 13, 2011 at the address indicated below and marked accordingly.

The Woodlands Township
2201 Lake Woodlands Dr
The Woodlands, Tx 77380
Attn: Carolyn Pennell
cpennell@thewoodlandstownship-tx.gov
281-210-3492
Re: Request for Proposals for Access Control and CCTV

The Township reserves the right to reject any and all responses resulting from this RFP. Late responses will not be accepted and will be returned to the submitting company unopened. Incomplete responses will be deemed non-responsive and will be rejected from consideration. The Township is not liable for any cost incurred by any person or firm responding to this RFP.

Please direct all questions regarding this RFP and the program it represents, in writing, to:

Mr. William Pham
wpham@thewoodlandstownship-tx.gov
IT Director
The Woodlands Township
2201 Lake Woodlands Dr
The Woodlands, Tx 77380

Proposals must be submitted in the format outlined in this section. Provide three (3) copies of your response. Each will be reviewed to determine if it is complete prior to actual evaluation. The Township reserves the right to eliminate from further consideration any response, which does not follow the format or is deemed nonresponsive; however, The Township reserves the right to waive any irregularities or formalities.

1. **Table of Contents**
   Proposals shall include a table of contents properly indicating the section and page numbers of the information included.

2. **Executive Summary**
   Proposals shall include a concise abstract stating the respondent's overview of the project.

3. **Contractor Qualifications Data**

A. **Firm Profile**

Provide general information on the responding firm, including; name, business address, local telephone number, officers of the firm, and contact person for this project.

B. **Project Team**

Provide a list of the employees of the firm who will work on this project. A one-page resume including education, experience, and any other pertinent information shall be included for each key member of the project team.

C. **References**

Provide a minimum of five (5) references for systems design and installation projects with a minimum of three (3) references applicable to Government and/or Municipal projects that have incorporated Access Control and IP-CCTV systems in the last thirty-six (36) months. Each reference shall describe the services and equipment provided, project cost, and benefits to the owner. Provide the owner's name, address, telephone number, and contact person for each reference. References for projects where the responding firm was not the prime contractor are not acceptable.

D. **Litigation**

Provide a description of any litigation to which your firm has been a party in the last five years to the extent such litigation pertains to Access Control and CCTV systems design and installation projects involving your firm.

3. **Technical Approach**

A. **Proposed Scope of Work**

Project design and methodology including technical approach and understanding of the scope of the project.

1. Proposals must indicate a clear understanding of the scope of the work, including a detailed project plan for this project outlying major tasks and responsibilities, time frames, and staff assigned for each category of the scope of work identified above.

2. Proposed Access Control and CCTV – Provide details regarding the system design services offered directly provided by the respondent, and identify any related services required to be provided by others (including The Township, Kirksey Architecture or the General Contractor) for full completion of this work. Proposals shall clearly distinguish the Contractors' duties and responsibilities and those of The Township.

Absence of this distinction shall mean the Contractor is assuming full responsibility for all tasks.

3. Proposed Equipment –For all proposed equipment, respondent shall provide cut sheets of proposed equipment and proposed design elements to assist with understanding the proposed direction of the Access Control and CCTV system design.

4. Certifications Concerning Proposed Equipment - The respondent must include in its response to this section a letter which shall certify the firm's capability to provide, install, and warrant all Access Control and CCTV system design components proposed.

5. A manufacturer's warranty on all proposed equipment shall be provided. The warranty period shall begin on the completion date of the project. The Access Control and CCTV system design, installation practices, and operation and maintenance practices shall not void any manufacturer's equipment or system warranty.

B. **Project Time-Line**

Proposals must provide chronological time-line of each task or event and estimated required to complete the engagement.

C. **Oversight from Single Contractor**

1. The Township strongly desires to contract with a single firm to accomplish all work and/or services outlined in this Request for Proposal.
2. Any proposed subcontractors must be identified in the Proposal response.
3. Any work not conducted by the Contractor or his subcontractors must be disclosed.

D. **Project Management**

Indicate your firm's approach to managing the project. Include a resume of the project manager responsible for the project.

4. **Financial**

Rates and Fees

1. Provide a proposed fee schedule.
2. Expenses not specifically listed will not be considered reimbursable.
3. Include a breakdown of equipment and installation costs.

5**. Documentation and Training**

1.Provide detailed information on the system documentation, operation guides and training programs available to The Township personnel and staff.

6. **Evaluation of Proposals**

A. Evaluation Process

The Township will appoint a selection committee to formally evaluate each response. The evaluation process will grade the responses on merit and responsiveness. The evaluation process will include verification of references and project team members, confirmation of financial information and may include other information as directed by The Township.

B. Grading Format

Each section or subsection of the response will be considered a separate selection criterion and will be graded individually. All scores will be summed to give the grand total score. The maximum possible total score for the response is 100 points.

C. Point Values

Criterion	**Point Value**
Contractor Qualification Data	**30 Total Points**
Project Team	10
References	20
Technical Approach	**35 Total Points**
Proposed Scope of Work	20
Project Time-Line	5
Single Firm Overseeing Contract	5
Project Management	5
Financial	**25 Total Points**
Rates and Fees	25
Documentation & Training	**10 Total Points**
Documentation	5
Training	5
Request for Proposals Total	**100**

Scope of Work and General Project Specifications

I. General Requirements

1. **Code**

A. Contractors shall be required to comply with all state and local code requirements.

B. It is the contractor's responsibility to notify the Owner if any code requirements, in place when the project is awarded, differ from any information contained in this specification.

2. **Locations**

See accompanying drawings for device locations. Drawing notes were created with Adobe X, which is available at no cost on the Adobe website.

II. Equipment \ Installing Company

1. Equipment shall be non-proprietary and readily available to low voltage systems suppliers through local distribution channels.
2. Access equipment shall be Linear eMerge, networkable, browser based or approved equal.
3. Include an alternate indicating any allowance for existing locks, (20) HID readers, (16) RTE PIR Motion Sensors, (15) RTE Buttons and egress hardware.
4. Quote with proximity tags (fobs) in lieu of proximity cards. Fobs should be compact, attachable to key chains, using Wiegand technology. Include 250 Programmed HID Proximity Fobs.
5. CCTV equipment; clients existing CCTV system to be moved and re-installed. Additional cameras will be needed. Current CCTV system is the AXIS camera management 2.0 with Surveillance Manager 4.7, and includes (1) AXIS 213 camera and (10) AXIS 233 Cameras.
6. An alternate IP-CCTV proposal may be submitted, but shall comply with non-proprietary paragraph (A) above. Clearly note any improvements in performance, such as increased resolution.
7. The installing company shall possess and maintain a State License for the services being provided, all installers on the project shall be licensed and registered.
8. General contractor to run wiring to the devices, and provide 110V power as needed, and provide the outdoor poles for parking lot coverage.

9. Network connections, including Ethernet, POE, and Wifi, shall be provided at the device by the owner.

A. Access Control: Operational Architecture

The System shall be implemented through network appliance architecture with a three-tiered modular hardware hierarchy and embedded three-tiered software architecture.

1. Network

The network appliance shall be capable of running on an existing TCP/IP network and shall be accessible, configurable, and manageable from any network connected PC with a browser. Browser access for configuration and administration of the system shall be possible from a PC on the same subnet, through routers and gateways from other subnets, and from the Internet. Control and management of the system shall therefore be geographically independent.

IP video cameras, video storage subsystems, VoIP intercoms, and other network connected storage systems shall be usable by the system via TCP/IP communications over the network.

Security of the data communicated over the network to and from the browser, network controller, and nodes is protected by encryption (SSL 128-bit) and authentication (SHA-1).

No separate networking shall be required.

2. Hardware

At the top of the hardware tiers is the Network Controller. Embedded on the network controller are an operating system, a web server, security application software, and the database of personnel and system activity.

The middle hardware tier is the Network Node. The network node shall make and manage access control decisions with data provided by the network controller, and it shall manage the communication between the network controller and application blades connected to the system's inputs, outputs, and readers.

The bottom hardware tier is the Application Blades. Four unique application blades shall be available.

An Access Blade shall support two readers, four supervised inputs, and four relay outputs.

An Alarm Input Blade shall support eight supervised inputs.

A Relay Output Blade shall support eight relay outputs.

A Temperature Blade shall support eight analog temperature sensor inputs.

This modular design makes it possible, even during network downtime, for the system to continue to manage access control, and store system activity logs. When network connectivity is reestablished the system activity logs are automatically reintegrated.

Each eMerge MicroNode shall function as a node and as an access control blade. In addition each MicroNode shall support one temperature input.

No separate PC client or PC server hardware or software shall be required.

3. Software

The database tier shall use PostgreSQL. PostgreSQL is a full featured, high performance database management system that supports ODBC. This shall provide a small footprint, low administration, and high reliability relational database that is embedded without requiring the use of a separate PC server.

The web server tier shall be based on GoAhead's embedded web server. This shall provide a graphically rich security management application through a standard web browser.

The security application software tier contains the business logic. This application shall also be embedded on the network device and requires no additional memory or processing power.

This three tiered embedded software design runs within an embedded Linux operating system and shall require no client side software other than a web browser.

Only a browser, shall be required for a base system.

B. Functional Capabilities

The System shall integrate in the browser interface the access control, alarm monitoring, camera and video monitoring, intercom, and temperature monitoring applications. The system shall also maintain a database of system activity, personnel access control information, and system user passwords and user role permissions.

1. Access Control Features

Access control features shall include:

- Multiple access levels and cards per person.
- 128-bit card support.
- HID Proximity Fob support.
- Detailed time specifications.
- Multiple card formats for mixed card populations.
- Activation/expiration date/time by person with one minute resolution.
- Access level disable for immediate lockdown.
- Use of Threat Levels to alter security system behavior globally.
- Multiple holiday schedules.
- Timed unlock schedules.

- Scheduled actions for arming inputs, activating outputs, locking and unlocking portals.
- Card enrollment reader support.
- Photo ID creation support.
- Counted-use access control.
- Regional and Timed anti-passback.
- Occupancy control
- Mustering
- Dual reader portal support
- 26-bit Wiegand keypad PIN support for 4 or 6 digit PINs
- 8-bit and 4-bit burst keypad support for 4 or 6 digit PINs
- Integration with supported alarm panels.
- First-in unlock rule.
- Up to 60,000 person records.

2. Alarm Monitoring Features

Alarm monitoring features shall include:

- User interface securely access under encrypted password control.
- Integrated alarm monitoring and event management with alarm panels.
- Alerts delivered to browsers, email, and cell phones.
- System user permissions to grant whole or partial access to system resources, commands, and personal data.

3. Camera and Video Monitoring Features

Camera and video monitoring features shall include:

- Real time video monitoring displays, including multiple cameras simultaneously.
- Video switching based on access activity or event activation.
- Video Management System including digital recording of events.
- Support for multiple DVR and NVR systems.
- Multiple supported cameras.
- Recall of photo ID and real time image for comparison.
- Full monitoring through a web browser interface.
- Limited monitoring through a smartphone interface.
- System user permissions to grant whole or partial access to system cameras and video resources.

4. Security Database Features

Security database features shall include:

- SQL capability and ODBC compliance.
- LDAP integration for single-user logon authentication.
- Optional storage and recall of ID photos and personal/emergency data.
- An API for adding to, deleting from, and modifying the database.
- Storage of system user passwords and permissions.
- System user permissions to grant whole or partial access to system resources, and personal data.
- Pre-defined reports on system configuration, system activity history, and people.
- English-based query language for instant custom reports.
- Custom Report writer interface that allows the interactive creation of custom reports. Reports may be saved for later reuse. No third party software such as Crystal Reports shall be necessary.
- Periodic backup to onboard flash ROM and optional network attached storage (NAS), including FTP servers.
- Periodic archive creation for historical custom reporting and improved on-board database performance.

C. Part 1: System Architecture

1. Software Architecture

The System shall consist of a network device with a three tiered embedded software architecture.

The database tier uses PostgreSQL. PostgreSQL is a full featured, high performance database management system that supports ODBC. This shall provide a small footprint, low administration, and high reliability relational database without requiring the use of a separate server.

The web server tier shall be based on GoAhead's embedded web server. This shall provide a graphically rich security management application through a standard web browser.

The security application software tier contains the business logic. This application shall also be embedded on the network device and requires no additional memory or processing power.

This three tiered embedded software design runs within an embedded Linux operating system and shall require no client side software other than a web browser.

2. Hardware Hierarchy

The System shall be built with a three-tiered hardware hierarchy.

At the top tier is the network controller, which shall contain the database engine, web server, application software, and configuration data. It is at this level that System Users, through a browser interface, shall interact with the System, set configurations, monitor activities, run reports, and manage alarms.

At the second tier is the network node, an intelligent device with native TCP/IP support, which shall make and manage access control decisions.

At the third tier are the application extension blades. Each of these blades shall connect to and manage a set of inputs, outputs, readers, cameras, or temperature monitoring points.

The network device shall run on existing building TCP/IP networks and shall be configurable for access from separate subnets, through gateways and routers, and from the internet.

3. Network Architecture

The major components of the System shall be a Network Controller and Network Nodes. Both are solid-state (fixed storage with no spinning hard drives or fans) and connect to a common LAN or WAN and use TCP/IP communications. VoIP intercoms, IP video cameras, digital video storage subsystems, and data storage systems shall also be network connectable and the System shall communicate with them using TCP/IP over the network.

The system shall have resident on the network controller a Linux-based database (PostgreSQL) and a web server. The database shall be ODBC compliant, and the web server shall provide a graphically rich user application through a standard web browser.

The system shall be configurable to function and be administered on one subnet, across subnets and gateways, or from any remote site via the internet.

D. Part 3: Technical & Functional Specifications

1. System Overview

a) Design Elements

(1) Scalability

The system shall be scalable to support the growth of security system needs. Additional nodes can be added to a blade server network controller up to a maximum of 32 nodes. Additional nodes can be added to a 1U rack server network controller (eMerge Enterprise) up to a maximum of 64 nodes or Micronodes, and up to 256 nodes or Micronodes for the 2U rack server controller (eMerge Ultra). Each of the nodes can carry an additional seven application blades. It shall not

be necessary to reconfigure existing system resources when adding additional nodes, application blades and devices.

(2) Browser-based User Experience

The system shall be capable of being monitored, administered, and configured through a browser on any computer connected to the network. The web server on-board the network controller shall provide a rich graphic application for the management of the system.

b) System Capacities

The system shall have up to the following capacities for each **blade server network controller with solid-state drive**:

- Nodes/Micronodes 32
- Access control readers: 448 maximum, 140 certified
- Access cards: 60,000+
- Card formats 32
- Alarm input points: 500
- Control point outputs: 500
- Temperature monitor points: 500
- Elevators 128
- IP, DVR, and NVR cameras: limited only by license
- Online event history log: 4 to 10 million records

  (depending upon configuration and transaction types)
- Ethernet switch ports: 2
- Time specifications 512
- Time spec groups 64
- Time specs per group 8
- Threat Levels 8
- Threat Level Groups 32
- Holidays 30
- Access levels per person 16
- Cards per person 100
- Report Groups 50
- Camera Groups 50
- Concurrent system users 10

The System shall have up to the following capacities for each **rack server controller** (eMerge Ultra):

- Nodes/Micronodes 64 (256 for eMerge Ultra)
- Access control readers 1792 (3584 for eMerge Ultra)
- Access cards 150,000
- Concurrent system users 25
- Alarm input points 2000 (4000 for eMerge Ultra)

The System shall have up to the following single network node capacities although all maximums cannot be achieved at the same time:

- Application blades: 7
- Access control readers: 14
- Access levels 512
- Portals 14
- Portal groups 64
- Reader groups 128
- Input groups 64
- Output groups 64
- Elevators 16
- Floors 100
- Floor groups 64
- Alarm input points: 56
- Control point relay outputs: 56
- Temperature monitor points: 56
- Credential storage: 20,000
- Event log records: 27,000

(1) Date formats

The system shall support the use of globally appropriate date formats. The specific date formats available shall be:

- mm/dd/yyyy
- dd/mm/yyyy
- yyyy/mm/dd

The system user shall be able to switch between date formats through the application graphic user interface.

(2) Character Set Support

The System in English shall support the UTF-8 character set.

The System in Spanish and Italian shall support the ISO 8859-1 character set.

c) Online Documentation

The system shall have an online Help system to provide explanations and procedures for all monitoring, administrative, and system configuration and maintenance functions. The Help system shall have linked table of contents, a linked index, and frequently asked questions pages. Each topic shall also have links to related topics. The Help shall be printable.

The online documentation shall also include Setup and Installation Guides, Video Recorder Integration Guides, and Tech Notes on specific technical topics. These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.

The Help system shall also be available in a zip file format (xxx.zip) and it shall be possible to install the online Help system on any computer for purposes of reference and use by support personnel.

d) End-user Documentation

A printable end-user manual shall be available for use by system monitors and administrators. The end-user manual shall describe all monitoring and administrating functions of the system.

e) Threat Levels

The system shall include configurable and settable threat levels. A threat level or a change in threat level shall be capable of effecting a change in the behavior of the security system. The areas of security system behavior that threat levels can change are portal unlock behavior, alarm event actions, and the function of access levels. A system user shall be able to configure threat levels, define behavioral changes based on the system threat level, and set the current threat level. Threat levels shall also be changeable automatically in response to alarm events.

f) Alarm and Event Monitoring

- The system shall be capable of monitoring, prioritizing, and acknowledging alarms. It shall be possible to associate specific actions with each alarm event. These actions may include but are not limited to sending pages and emails, energizing outputs to activate lights, locks, or alarms, changing the system threat level, switching to an appropriate video monitor, displaying ID photos, and flashing device icons on a graphic floor plan, positioning a PTZ camera, and recording video.
- Access not completed for <username> at <portalname>

(1) Cameras

The system application shall provide a pick list of all configured IP, DVR and NVR cameras. The user may also create a favorites folder for

specific cameras. When selected the application shall provide a page for display of the camera monitor. That page shall also provide controls for Pan, Tilt, and Zoom camera telemetry, and for selecting preset positions on the camera website.

The system shall support user-definable camera types.

It shall also be possible to create a thumbnail monitor of the current camera image. This thumbnail image shall be live and shall remain displayed on the screen until dismissed. Use of other applications and other functions of the security system application shall be possible while maintaining the thumbnail camera monitor display.

g) Access Control

The primary purpose of the system is to provide access control. The system shall be able to make access control decisions, define a variety of access levels and time specifications, write system activity into a log file, maintain a personnel enrollment database, receive signals from input devices such as door switch monitors, card readers and motion detectors, energize devices such as door locks and alarms via outputs, and provide on-screen monitoring features.

The System User, holding at least a “Setup” user role, shall be able to create, delete, and edit access control specifications and configurations.

(1) Time Specifications

The system shall be capable of storing up to 512 time specifications. Each time specification must be assigned a unique alphanumeric name of up to 64 characters. The definition of a time specification shall require the assignment of both a start time and an end time. Each day of the week shall be individually assignable for inclusion in time specifications. Up to three holiday groups shall be assignable for inclusion in time specifications. If no holidays are assigned to a time specification then no holiday access shall be allowed.

Time specifications shall be assignable to access levels, output groups, portal groups, input groups, and alarm events.

Time specifications shall function appropriately per node for the time zone specified for that node.

(2) Time Specification Groups

It shall be possible to create groups of time specifications for the purpose of creating complex time specifications. The system shall be capable of storing up to 64 time specification groups with up to 8 time specifications per group.

(3) Card Formats

The system shall support the use of readers that use the Wiegand Reader Interface. The system shall default to the Wiegand 26 bit

format unless a different bit length format is created in the system. The system shall support but not require the use of the card facility code.

The system shall support the use of HID Proximity Fobs.

The system shall also support the use of the Magnetic Stripe ABA track 2 card data formats.

The system shall be preloaded with six popular access card formats.

It shall be possible to create new card formats, designate start bits and bit lengths for facility codes and card ID numbers, as well as designate parity bits. The system shall support up to 32 different card formats. The system shall support card formats up to 128 bits.

(4) Access Levels

The system shall be capable of storing up to 512 access levels. Each access level must be assigned a unique alphanumeric name of up to 64 characters. The definition of an access level shall require the assignment of a reader or reader group, and a time specification. It shall be possible to also assign an elevator floor group to an access level.

Up to 16 access levels shall be assignable to any person ID in the system.

(5) First in Unlock Rule

The system shall support the use of a first in unlock rule. It shall be possible to use this rule to control the unlock behavior of portal groups with assigned unlock time specs. The unlock rule shall require a card read of a specified access level. The portals in the group shall unlock only when the First-in Unlock rule is satisfied and the unlock time spec is valid.

(6) Holidays

The system shall be capable of storing up to 30 holidays. Each holiday must be assigned a unique alphanumeric name of up to 64 characters. The definition of a holiday shall require a start date and an end date. Holiday definitions shall support the designation of a start time and an end time. If no start time is designated then the system shall default to 00:00 (start-of-day). If no end time is designated then the system shall default to 24:00 (end-of-day). Holidays shall require the use of 24-hour time format, e.g. 17:00 is 5:00PM.

Holidays can be assigned to up to three holiday groups. The system shall support the use of a pop-up calendar from which System Users can select dates for holidays.

(7) Portals

A portal is any access point and each portal supports up to 2 access reader devices. The System User, holding at least a “Setup” user role,

shall be able to view current portal definitions, change portal definitions, delete portals, and create new portal definitions. Creating a portal defines the access and alarm behavior of the access point. This can include:

- card readers and keypads
- an output for locking
- an input for monitoring the door switch (DSM)
- an input for the Request-to-Exit (REX) function
- local alarm outputs and system alarm events.

(a) Portal Required Information

Portal name and node address shall be the only required fields in a portal definition. However, for a portal to function for access control it shall be necessary to assign at least a reader and lock output.

(b) Portal Alarm Conditions

Portals shall have four alarm conditions. The four alarm conditions are as follows:

1. Forced: When a portal is opened and there has been no card read, nor request to exit.
2. Held: When a portal is held open past the expiration of the shunt timer.
3. Invalid: When the portal reader reads a card for which there is no entry in the database.
4. Valid: When the portal reader reads a card for which there is a valid entry in the database.

(c) Unlock, Request to Exit Modes

- Unlock Time: Unlock duration, set using seconds, shall be settable and editable. It shall also be possible to set an extended unlock time for ADA compliance (Americans with Disabilities Act).
- Shunt Time: Shunt time duration, set using seconds, shall be settable and editable. It shall also be possible to set an extended shunt time for ADA compliance (Americans with Disabilities Act).
- Relock on open: It shall be possible to set portals to relock immediately once opened.
- Unlock on Rex: It shall be possible to set portals to unlock when a REX is initiated.
- REX Mode: The Request to Exit mode shall be settable to either motion mode (motion detection) or push mode (manual switch). Once a REX is initiated alarms are

suppressed for the duration of the shunt timer, allowing the individual to exit without triggering an alarm.

- Accept read while open: It shall be possible to set portal readers to accept card reads while the door is open. Unless this is set, portal readers will not accept card reads until the door is closed.

(d) Portal Alarms

- Local to Node: Output responses to alarm states shall be settable for any of the four portal alarm conditions: Forced, Held, Valid, and Invalid. Outputs shall be selectable from dropdown lists for each condition and the duration of the output function shall be settable in seconds. These responses to alarm conditions shall be managed by the node and shall not require network connectivity. These events shall not be logged in the system activity database.
- Alarm Events: Alarm events shall be assignable to each of the four portal alarm conditions: Forced, Held, Valid, and Invalid. Events shall be selectable from dropdown lists for each condition and it shall be possible to enable or disable these events using a checkbox without un-assigning or reassigning events. These events can include multiple actions and shall be logged in the system activity database.

(e) Portal Groups

It shall be possible to create groups of portals and to assign an unlock time specification to the entire group. All the portals in the group shall remain unlocked during the time specified.

It shall also be possible to assign a group of threat levels to a portal group. An unlock time specification will function to unlock the portals in the group only if the current system threat level is one of the threat levels assigned to the portal group.

It shall be possible to use portal groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If a portal group is assigned to a particular system user then the portals in that group shall be viewable and unlockable by that system user.

(f) Portal Readers

It shall be possible to assign two readers to a portal. The reader(s) and portal must both be on the same node. The reader(s) shall send card data to the node whenever a card read is performed.

(g) Reader Definitions

The only required entry for a reader shall be a name. However, it shall be necessary to designate a node, slot and position for the reader if it is to function as part of a node or access level definition. It shall also be possible to enter a text description of the reader. The reader definition screen shall display names of all reader groups that contain that reader. It shall not be possible to delete a reader if it is part of a reader group or access level. A checkbox shall be provided to enable or disable the reader without having to delete or alter its definition.

h) Reports

The system shall be capable of producing a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system. In addition, an easy to use query language shall be included for the use of the System User in creating ad hoc reports. The query language shall be documented in an on-line help system. Alternatively, it shall be possible to specify a query by use of point-and-click.

It shall also be possible to produce reports directly from the IEI eMerge based on data in archive files on FTP servers, network attached storage, or the controller-attached compact flash.

The system shall support a graphic interface for interactively building custom reports from either historical or personnel data. These reports shall be savable for later reuse. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a pdf file or put into a spreadsheet.

It shall also be possible to group reports for assignment to custom user roles. Any reports not grouped and assigned to a custom user role shall not be viewable by that system user.

Report generation shall not affect the real-time operation of the system.

The specific reports provided shall include the following:

(1) Configuration Reports

As Built: A graphical report that documents all resource connections to the system.

Cameras: Displays all camera configuration information including control address, IP port, and camera type.

Camera Presets: Displays configured presets for each camera in the system.

Elevators: Displays elevator configuration information including Node, Reader, and Floor to output mappings.

Floor Groups: Displays all configured floor groups for use in elevator control.

Holidays: Displays holiday specification information.

Portals: Displays portal definition information including reader, DSM input, REX input, alarm outputs, and events.

Portal Groups: Displays a list of all defined portal groups.

Reader Groups: Displays defined groups of readers.

Resources: Displays all configured system resources including readers, inputs, outputs, elevators, and temperature points.

Threat Level Groups: Displays all configured threat level groups and the threat levels assigned to them.

Threat Levels: Displays all configured threat levels including the description and color assignment.

(2) History Reports

Access History: Displays access history based on an entered query. The system user can specify the query using either the keyboard or point-and-click selection.

Custom Report: This provides the capability to create custom reports of historical data. Reports may span the dates of the active database as well as any applicable archive database files. The use of archive database files to satisfy report queries shall be automatic. A graphic interface provides the user with the ability to interactively create and save reports for later use. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a pdf file or put into a spreadsheet.

General Event History: Displays time, type of activity, and activity details for a variety of event types. The System User can select the specific event types for the report.

Portal Access Count: Display how many times users have used a portal.

(3) People Reports

Access Levels: Displays all access levels entered into the system including time specification, reader/reader group, and floor group.

Current Users: Displays a list of all security system users currently logged in to the security system website.

Custom Report: This provides the capability to create custom reports of personnel data. A graphic interface provides the user with the ability to interactively create and save reports for later use. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a pdf file or put into a spreadsheet

Occupancy: Displays a list of defined regions with the number of people currently occupying each region and the maximum number of occupants allowed, if a maximum has been specified.

Photo ID Gallery: Displays all the photo ID pictures in the system and the person's name.

Photo ID Requests: Displays all outstanding badge print requests and lists ID, name, badge layout, activation date, request date.

Portal Access: Lists people with access for a selected portal.

Roll Call: Allows you to select a defined Region from the drop-down and see a list of people currently in that region.

Roster: Displays every person entered into the system and it lists name, ID photo, expiration date, username, and access level.

Time Specifications: Displays all defined time specifications currently in the system.

i) Network TCP/IP based Live Video Surveillance

The system shall provide live IP video surveillance capability. The number of supported cameras shall be limited only by license. The system's video capabilities shall include video monitor switching based on access activity. The system shall provide monitoring, configuration, and administration of IP video. Cameras can be separately monitored or monitored in groups.

The system shall support IP video cameras from multiple manufacturers for live view.

(1) Definitions

The system shall support the naming and definition of IP cameras. Required data for defining a camera shall include:

- Name
- Browser IP Address
- Control IP Address
- IP Port
- Camera Type

(2) Menu Order

The application shall provide a page for setting the order of the configured cameras on menus and pick lists.

(3) Presets

The system shall support the creation, deletion, and editing of camera preset positions in the system. It shall also be possible to save changes in preset positions directly to a camera website.

Camera preset positions must first be set at each camera web site. For setting up camera presets in the system it shall be necessary to enter the preset name and preset number exactly as it is entered on the camera's web site.

The application shall provide a toggle for designating a home preset position.

(4) Types

The system shall support IP video cameras from multiple manufacturers. The application shall provide a drop down pick list for selecting the camera type or creating a new type. Motion JPEGs shall be supported.

The application shall provide fields for entering and editing camera command URLs. The command URLs that the application shall support include:

- Pan/Scan URL
- Pan URL
- Tilt URL
- Pan Tilt URL
- Zoom URL
- Preset URL
- Brightness URL
- Image URL
- Motion JPEG URL
- Assign Preset URL

(5) Views

The system shall support the creation, deletion, and editing of multiple camera views, specifically Quad views (four cameras), and picture-in-a-picture (two cameras).

The application shall provide a drop down pick list for selecting current views or naming of new views. The application shall also provide a drop down pick list for the selection of the view type.

The application shall provide a pick list for selecting individual cameras for inclusion in a view.

j) System Administration

The system shall provide for the performance of system administration tasks from any network-connected computer with a browser. These administrative tasks shall include but not be limited to database backups, software updates, file cleanup, and configuring network resources. Most of the administrative, maintenance, and configuration utilities and functions

shall require a system user with at least a “Setup” user role. Information from the network administrator shall, in many cases, also be required.

(1) Network Architecture

The system shall be capable of running on an existing TCP/IP network and shall be accessible, configurable, and manageable from any network connected PC with a browser. Browser access for configuration and administration of the system shall be possible from a PC on the same subnet, through routers and gateways from other subnets, and from the Internet. Control and management of the system shall therefore be geographically independent.

(2) Database and Full System Backups

The system shall create database, or full system data backups each night at 00:15 hours. These backups shall be stored in ROM and compact flash onboard the solid-state network controller, and written to the drive on the disk-based controller.

Backups shall also be written to network attached storage (NAS) or an FTP server if such storage has been configured in the system.

It shall also be possible for the system users to create such database backups at any time. Any database backups onboard the network controller may also be downloaded to off board storage by the system user at any time.

(3) Database and Full System Restore

The system shall be able to restore its database, or the full system data, from a backup. Restoration of the system shall only be possible from a backup copy onboard the network controller. It shall, therefore, be possible to upload a copy of a database backup from any network attached storage.

It shall be possible to review backups by date and description and select the desired backup for upload to the network controller or restoration as the current system database.

(4) FTP Backup

The system shall support the use of an FTP Server for backups. Once configured, backups are automatically saved to the FTP server each night.

It shall also be possible to setup NAS servers for backup storage.

(5) Defining Network Attached Storage (NAS) for Backup

The system shall support the use of network attached storage devices for backups. The network administrator must create a domain user account for the network controller and a password. The system user must configure the network attached storage in the system including

the domain name, server IP address, share name, and the directory where the network controller may store data.

The system shall use the configured network attached storage for database backups, ID photos, database archives, and software updates.

It shall also be possible to setup FTP servers for backup storage.

(6) System Archives

The system shall periodically create archive files for historical custom reporting and improved on-board database performance. It shall be possible to store archive files both on the system and off the system on NAS and FTP servers.

(7) Badge Design and Printing

The system shall include an integrated badging function. It shall be possible to design badge layouts, upload badge layouts for badge printing, capture ID photo images, print badges, and delete uploaded badge layouts.

It shall be possible for the system user to manage all badging functions entirely from within the browser.

(8) Card Format Decoding

The system shall include a card format decoding utility that presents a graphical view of the data on each card and assists in the discovery of card numbers, facility codes, and formats. This card decoder shall decode both Wiegand and ABA track 2 data formats.

(9) Upgrades and Patches

Software updates, upgrades and patches shall be provided from time to time. The system shall be able to update its software from these .tgz files. Update of the application software shall only be possible from an update file onboard the network controller. It shall, therefore, be possible to upload a copy of the software update from any network attached storage or from any PC drive or desktop.

Software updates may involve the network controller only or may include updates for the node(s) also. The monitoring of the security system may be unavailable for several minutes during this process.

(10) File Cleanup

A utility shall be provided to assist in file cleanup. This utility will display for review and deletion all floor plan jpeg files, photo IDs, database backups, badge layouts, and software updates.

(11) System Shutdown

A utility shall be provided to perform an orderly system shutdown. The current security database will be stored onboard in ROM. The system

will remain stopped until power is removed and reconnected. When the system reboots the security database image in ROM is read and used as the current database.

This function is intended for use when physically moving the system or performing hardware service requiring the disconnection of power.

(12) System Reboot

A utility shall be provided to perform a system reboot. Before the system shuts down it will store the current security database in ROM. When the system comes back up the security database image in ROM is read and used as the current database.

(13) Network Node Refresh

A utility shall be provided to refresh security database and configuration data to all nodes. Nodes will normally be refreshed automatically whenever the network controller has new data. However, it will be possible to force an immediate refresh of node data after changes have been made to the security database or configurations.

(14) Test Network Connection

A utility shall be provided to ping a known network IP address to check for connectivity between the security system network controller and other network devices.

(15) Reset AlarmTables

A utility shall be provided to reset all alarms and clear all event actions. Normally this should not be necessary. However, If an alarm persistently reappears then the alarm inputs involved should be investigated as they may have wiring problems. In such a case the system user may need to clear all alarms.

(16) Repair Database Tables

It shall be possible for a system user to execute a MySQL Repair Database Tables command. This command is designed to repair some data table corruptions that can occur.

(17) Email Settings

The system shall support the use of email notifications of alarm events. The system user must setup the email server IP address or DNS name and the email address of the network controller. A network administrator must setup the network mail server to relay email for the IP address of the network controller.

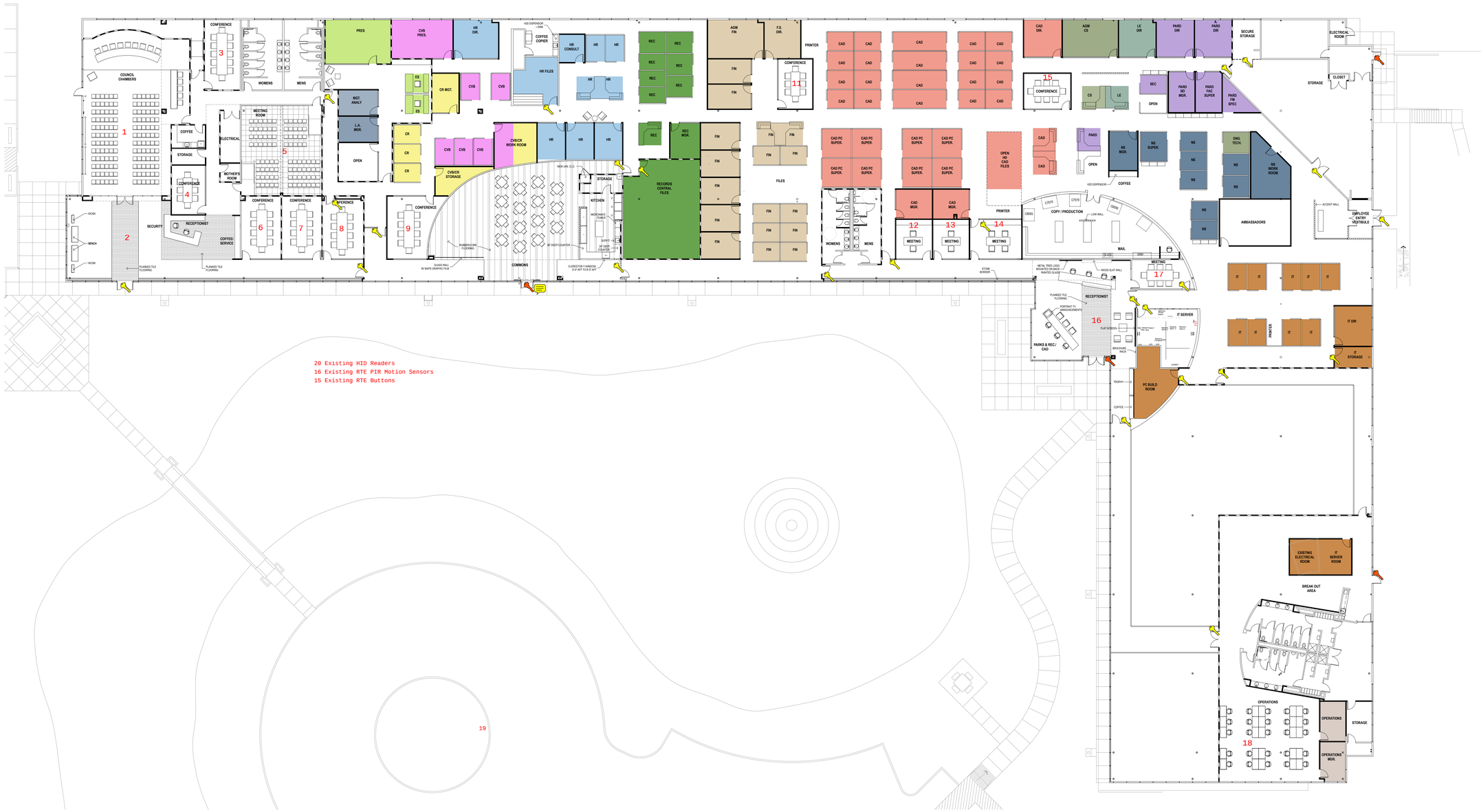
(18) Setting Time Zone, Time Servers, and System Time

The system shall support the setting of time zones by selection off of a drop down pick list. Time zones shall be separately settable for the controller and for each node or MicroNode in the system. An extensive list of world-wide time zones shall be provided. Adjustments for daylight saving time (summer time) shall be automatic.

The system shall support the use of network time servers. Up to three time servers can be designated. Use of a network time server ensures that the network controller and its nodes will be regularly synchronized with the exact time used by all other network resources.

It shall also be possible to manually set the system date and time.

Attachment A-Access



Attachment B- Building Cameras

= Fixed cameras, network attached to existing AXIS system. May include and alternate quote for megapixel cameras, up to 2MP. Specify resolution in proposal whether mega pixel or non-mega pixel for comparison purposes.

Attachment C-Parking Lot Cameras

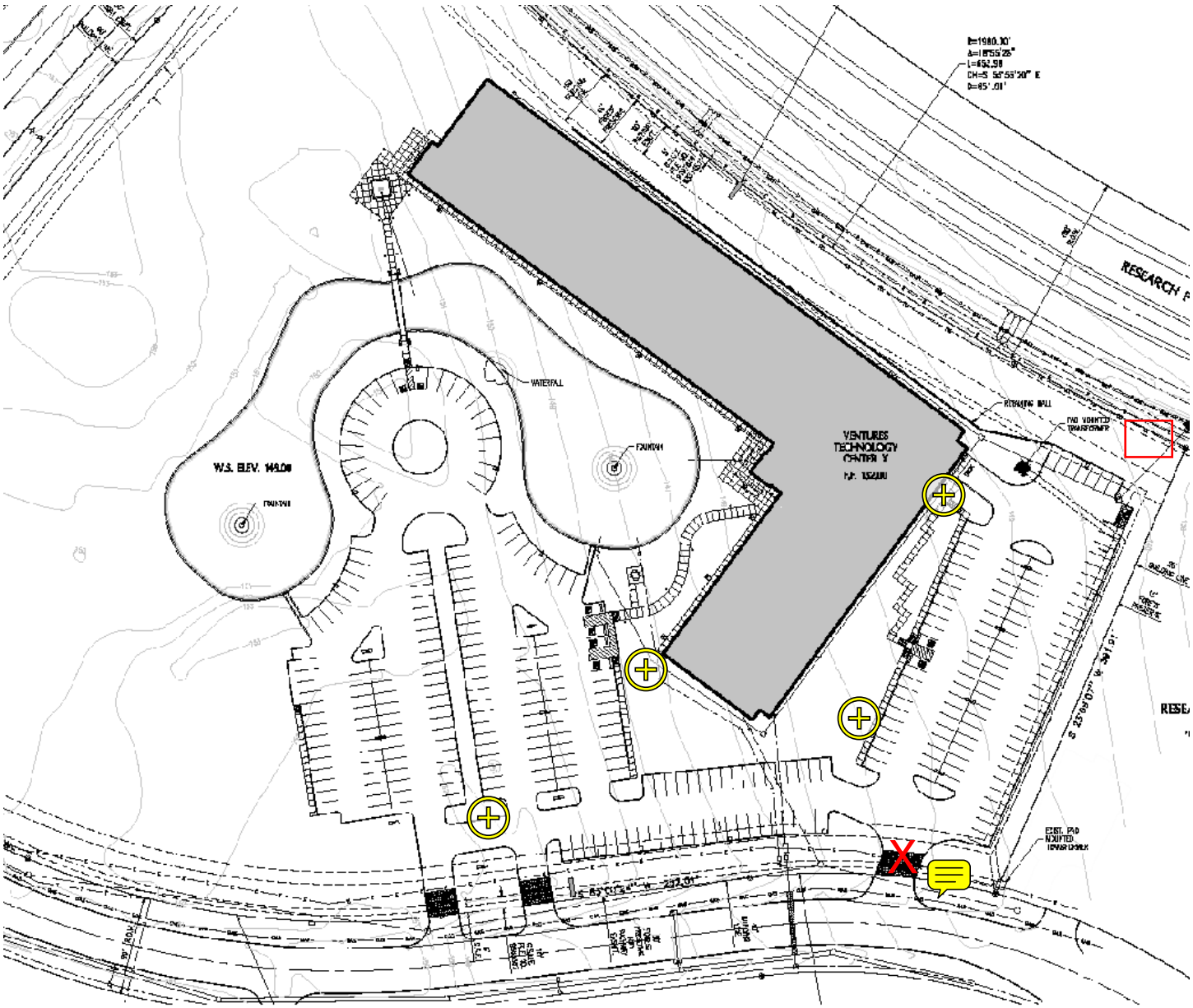


EXHIBIT "B"

FLOOR PLAN OF PREMISES